UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN
AT LAW AND IN ADMIRALTY

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No.

APPROXIMATELY 114,366.044785 TETHER (USDT) CRYPTOCURRENCY FROM BINANCE ACCOUNT USER ID ENDING IN 7382,

APPROXIMATELY 2,155,760.485382 TETHER (USDT) CRYPTOCURRENCY FROM CRYPTOCURRENCY ADDRESS ENDING IN Mbc25MQY, and

APPROXIMATELY 3,314,499.122779 TETHER (USDT) CRYPTOCURRENCY FROM CRYPTOCURRENCY ADDRESS ENDING IN XkPYyCSJ,

Defendants.

VERIFIED COMPLAINT FOR CIVIL FORFEITURE IN REM

The United States of America, by its attorneys, Gregory J. Haanstad, United States Attorney for the Eastern District of Wisconsin, and Elizabeth M. Monfils, Assistant United States Attorney for this district, alleges the following in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

Nature of the Action

1. This is a civil action to forfeit properties to the United States of America, under 18 U.S.C. §§ 981(a)(1)(A) and 984 and 21 U.S.C. § 881(a)(6), for violations of 18 U.S.C. §§ 1956, 1957, and 1960 and 21 U.S.C. §§ 841(a) and 846.

The Defendants In Rem

2. The defendant property, approximately 114,366.044785 Tether (USDT)[1] cryptocurrency from Binance account user ID ending in 7382, held in the name of an individual having the initials J.M.U.L., was seized on or about July 9, 2024, in San Francisco, California.

3. The defendant property, approximately 2,155,760.485382 Tether (USDT) cryptocurrency from cryptocurrency address ending in Mbc25MQY, was seized on or about July 29, 2024, in Road Town, Tortola, British Virgin Islands.

4. The defendant property, approximately 3,314,499.122779 Tether (USDT) cryptocurrency from cryptocurrency address ending in XkPYyCSJ, was seized on or about July 29, 2024, in Road Town, Tortola, British Virgin Islands.

5. The Drug Enforcement Administration seized the defendant property, approximately 114,366.044785 Tether (USDT) cryptocurrency from Binance account user ID ending in 7382, pursuant to seizure warrant 24-MJ-149 issued by United States Magistrate Judge William E. Duffin in the Eastern District of Wisconsin on July 9, 2024.

6. The Drug Enforcement Administration seized the defendant property, approximately 2,155,760.485382 Tether (USDT) cryptocurrency from cryptocurrency address ending in Mbc25MQY, pursuant to seizure warrant 24-MJ-164 issued by United States Magistrate Judge William E. Duffin in the Eastern District of Wisconsin on July 29, 2024.

7. The Drug Enforcement Administration seized the defendant property, approximately 3,314,499.122779 Tether (USDT) cryptocurrency from cryptocurrency address

[1] Tether, often referred to by its currency code of USDT, is a stablecoin cryptocurrency with a value meant to mirror the value of the U.S. dollar. USDT tokens are backed by offshore banks. Offshore banks offer fewer charges for operation and tax benefits, but they are not always fully secure like the FDIC-insured U.S. banks.

ending in XkPYyCSJ, pursuant to seizure warrant 24-MJ-165 issued by United States Magistrate Judge William E. Duffin in the Eastern District of Wisconsin on July 29, 2024.

8. The defendant properties are presently in the custody of the United States Marshal Service in Arlington, Virginia.

Jurisdiction and Venue

9. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a).

10. This Court has *in rem* jurisdiction over the defendant properties under 28 U.S.C. § 1355(b).

11. Venue is proper in this judicial district under 28 U.S.C. § 1355(b)(1) because the acts or omissions giving rise to the forfeiture occurred, at least in part, in this district.

Basis for Forfeiture

12. The defendant property, approximately 114,366.044785 Tether (USDT) cryptocurrency from Binance account user ID ending in 7382, is subject to forfeiture under 21 U.S.C. § 881(a)(6) because it represents proceeds of distribution of controlled substances and a conspiracy to distribute, manufacture, dispense, or possess with the intent to manufacture, distribute, or dispense controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846.

13. The defendant property, approximately 114,366.044785 Tether (USDT) cryptocurrency from Binance account user ID ending in 7382, is also subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 984 because (1) it was involved in, or is traceable to funds involved in, money laundering transactions and a conspiracy to engage in money laundering in violation of 18 U.S.C. §§ 1956 and 1957; and (2) it was involved in, or is traceable to funds involved in, unlicensed money transmitting in violation of 18 U.S.C. § 1960.

14. The defendant property, approximately 2,155,760.485382 Tether (USDT) cryptocurrency from cryptocurrency address ending in Mbc25MQY, is subject to forfeiture under 21 U.S.C. § 881(a)(6) because it represents proceeds of distribution of controlled substances and a conspiracy to distribute, manufacture, dispense, or possess with the intent to manufacture, distribute, or dispense controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846.

15. The defendant property, approximately 2,155,760.485382 Tether (USDT) cryptocurrency from cryptocurrency address ending in Mbc25MQY, is also subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 984 because (1) it was involved in, or is traceable to funds involved in, money laundering transactions and a conspiracy to engage in money laundering in violation of 18 U.S.C. §§ 1956 and 1957; and (2) it was involved in, or is traceable to funds involved in, unlicensed money transmitting in violation of 18 U.S.C. § 1960.

16. The defendant property, approximately 3,314,499.122779 Tether (USDT) cryptocurrency from cryptocurrency address ending in XkPYyCSJ, is subject to forfeiture under 21 U.S.C. § 881(a)(6) because it represents proceeds of distribution of controlled substances and a conspiracy to distribute, manufacture, dispense, or possess with the intent to manufacture, distribute, or dispense controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846.

17. The defendant property, approximately 3,314,499.122779 Tether (USDT) cryptocurrency from cryptocurrency address ending in XkPYyCSJ, is also subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 984 because (1) it was involved in, or is traceable to funds involved in, money laundering transactions and a conspiracy to engage in money laundering in violation of 18 U.S.C. §§ 1956 and 1957; and (2) it was involved in, or is traceable to funds involved in, unlicensed money transmitting in violation of 18 U.S.C. § 1960.

Facts

18. Cocaine is a Schedule II controlled substance under 21 U.S.C. § 812.

Background

19. Drug trafficking organizations ("DTOs") generate large amounts of cash proceeds in the United States and elsewhere. In order to repatriate their cash proceeds from the United States and other countries back to their country of origin where they can be used by the DTO members, DTOs often employ professional money launderers. For a fee, professional money launderers provide the DTO with currency in the DTO's native country in exchange for bulk currency in the country where the DTO's narcotics are distributed.

20. Professional money launderers use a variety of methods to accomplish their goals, including trade-based money laundering, bulk currency smuggling, and virtual currency trading.

21. Virtual currency, also known as cryptocurrency, is generally defined as an electronically sourced unit of value that can be purchased with, sold for, or used as a substitute for fiat currency (i.e., currency created and regulated by a government). Cryptocurrency is not issued by any government, bank, or (with limited exceptions) companies. It is instead generated and controlled through computer software operating on a decentralized peer-to-peer network.

22. Cryptocurrency can be quickly transmitted directly between parties and across national borders, without the need for a facilitating third party like a traditional financial institution. Many cryptocurrencies, including Bitcoin and Tether, operate via a "blockchain," a record (or ledger) of every transaction ever conducted that is distributed throughout the network. The blockchain will not list the names of parties to the transaction but will list the date and time of the transaction, the originating and receiving public address, and how much cryptocurrency was transferred.

23. Based on their training and experience, and their knowledge and information garnered from money launderers in this case and similar cases, agents know that cryptocurrency transactions are often used to launder the proceeds derived from narcotic traffickers. More specifically,

A. Narcotics traffickers in source countries (e.g., Mexico and Colombia) provide narcotics to consumer countries (e.g., the United States).

B. The bulk currency proceeds derived from the sale of these narcotics are then returned to the narcotics traffickers within the source countries using various methods, including the use of cryptocurrencies. In this case, the narcotics traffickers often contacted brokers, or professional money launderers, who were responsible for collecting the bulk currency within the consumer countries and depositing the currency into the U.S. banking system.

C. The brokers often then paid out the narcotics traffickers in fiat currency within the source countries, minus a commission, and sold the cryptocurrency to a separate "crypto" broker. The commission fee was generally between three percent and five percent.

D. The cryptocurrency broker may have then conducted a series of cryptocurrency transactions across multiple cryptocurrency exchanges using an array of methods (e.g., cryptocurrency scrambler) in an effort to obfuscate the true origin of the money. The cryptocurrency brokers often then sold the cryptocurrency in the "black market" in exchange for various fiat currencies.

International drug trafficking and money laundering organization

24. In August 2020, agents received a tip regarding possible international drug trafficking and tax evasion. The tip included, in part, the following information:

A. An individual having the initials D.C. was identified as one of the persons involved in drug trafficking.

B. D.C. had been imprisoned for federal drug charges in the past.

C. D.C. was living a lavish lifestyle, clearly beyond D.C.'s means.

D. Individuals involved in drug trafficking were using a business called S&C Trucking LLC, 1XXX East Lafayette Place #3XX, Milwaukee, Wisconsin,[2] to hide drug proceeds.[3]

E. D.C. operated S&C Trucking LLC located in Milwaukee, Wisconsin. The business was registered with the DOT [Wisconsin Department of Transportation] under a different address that is a home, but it actually operated at 5XXX West Clinton Avenue, Milwaukee, Wisconsin.

25. According to Wisconsin Department of Financial Institutions records, D.C. was the registered agent of S&C Trucking LLC. The address listed for the business was 9XXX West Tower Avenue, Milwaukee, Wisconsin (the "Tower Avenue residence"). Agents conducted surveillance at the Tower Avenue residence on several occasions and never saw a person or vehicle come or go from the residence. Agents also observed that cameras were mounted on the exterior of the Tower Avenue residence, and that all of the window blinds of the residence were closed.

26. Based on their training and experience, agents know that drug traffickers frequently maintain "stash" houses, which are residences used to store drugs before distribution and/or to store proceeds of drug sales after distribution. These residences typically have little vehicle or pedestrian traffic to avoid drawing attention to the house. In addition, cameras are often mounted to the exterior of "stash" houses to allow the drug traffickers to observe whether the residence was being approached by law enforcement or by rival drug traffickers.

27. On October 20, 2020, Texas Department of Public Safety investigators were conducting surveillance at a suspicious business in Pharr, Texas. An overhead garage door at the business warehouse was open and investigators saw a pallet containing several boxes sitting next to a pickup truck in the business. The rest of the warehouse appeared to be empty.

[2] This address is for a condominium unit.

[3] Throughout this complaint, certain information has been redacted using the letter "X" as a means of avoiding the revelation of any personal information.

A. A truck belonging to Estes Express Lines arrived, loaded the pallet onto the truck, and left the business. Investigators maintained surveillance on the truck until it arrived at the Estes Express Lines property.

B. Investigators approached the employees of Estes Express Lines and inquired about the pallet. Employees provided investigators with the bill of lading related to the shipment. The bill of lading indicated that the pallet contained 492 pounds of optical cable and was being shipped from Dixie Cable, 2003 North Veterans Boulevard, Suite 18, Pharr, Texas, to an individual having the initials R.G. at 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin. The shipper name was listed as an individual having the initials C.T. with phone number (956) 996-2XXX. The recipient was listed as R.G. with phone number (657) 261-1XXX.

C. A drug detection canine gave a positive alert to the odor of a controlled substance on the pallet. Investigators searched the pallet and found approximately 60 kilograms of cocaine concealed within the boxes on the pallet.

28. According to shipping records, three prior shipments had been sent from Pharr, Texas, addressed to 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin. Two of those shipments had been picked up at the shipping company's location in Milwaukee, Wisconsin. One shipment was delivered to 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin on August 14, 2020. Surveillance regarding the August 14, 2020, shipment revealed the following:

A. Surveillance video from North Shore Bank[4] showed that on August 14, 2020, D.C. arrived at the side of the business located at 1850 North Martin Luther King Jr. Drive in a black Dodge Ram 2500 pickup. The bed of the pickup was empty upon D.C.'s arrival.

B. A short time later, a box truck driven by the shipping contractor arrived and parked on the side of the business.

C. D.C. positioned the Dodge Ram near the shipping company vehicle.

D. A short time later, D.C. drove away from the area. The bed of the Dodge Ram now contained what appeared to be a shipping pallet containing several

[4] North Shore Bank is located at 1900 North Doctor Martin Luther King Jr. Drive, Milwaukee, Wisconsin, which is across the street from 1850 North Martin Luther King Jr. Drive, Milwaukee, Wisconsin.

cardboard boxes. This pallet was similar in appearance to the pallet seized in Pharr, Texas, on October 20, 2020.

29. Wisconsin Department of Financial Institutions records showed that Peachy Clean Commercial and Construction Cleaning LLC listed its office address as 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin. The registered agent was an individual having the initials R.T. Numerous law enforcement database searches identified R.T.'s phone number as (414) 803-9XXX.

30. AT&T records related to phone number (414) 469-6XXX show the subscriber as D.C. at 9XXX West Tower Avenue, Milwaukee, Wisconsin (the Tower Avenue residence).

A. Phone records for (414) 469-6XXX further show that D.C. was in contact with (414) 803-9XXX, the number used by R.T., 153 times from March 5, 2020, through October 8, 2020.

B. Phone records for (414) 469-6XXX further show that D.C. was in regular and frequent contact with other phones known to be used by drug traffickers in the Milwaukee, Wisconsin, area.

31. On November 2, 2020, the Honorable William E. Duffin, United States Magistrate Judge in the Eastern District of Wisconsin, signed a tracking warrant for a silver 2015 Kia Optima, bearing Wisconsin license plates ACV-2XXX (the "Kia"), known to be driven by D.C.

32. On November 24, 2020, agents saw that the Kia left the Tower Avenue residence and traveled directly to a vacant lot in the 4700 block of South Packard Avenue, Cudahy, Wisconsin. Agents responded to that area to conduct surveillance of the Kia.

A. At approximately 3:27 p.m., agents saw that the Kia travelled to the parking lot of a BMO Harris Bank located at 4677 South Packard Avenue, Cudahy, Wisconsin.

B. Agents conducted surveillance of the Kia and saw D.C. in the driver's seat and an unidentified male in the front passenger seat. The unidentified male appeared to be looking down at the passenger-side floorboard.

C. At approximately 3:35 p.m., the Kia drove out of the BMO Harris parking lot and drove back to the 4700 block of South Packard Avenue. The Kia did a U-turn and pulled to the curb on the south side of the street. The unidentified male exited the front passenger seat and retrieved a small rolling suitcase and a small duffel bag from the vehicle. The unidentified male then entered the JP Morgan Chase Bank at 4702 South Packard Avenue, Cudahy, Wisconsin. D.C. then drove the Kia out of the area.

D. Inside JP Morgan Chase Bank, the unidentified male approached a teller window and appeared to be conducting a lengthy transaction. At approximately 4:34 p.m., the unidentified male exited the bank and stood in front of the bank looking at his cellular phone.

E. At approximately 4:42 p.m., a vehicle displaying an Uber sticker arrived in front of JP Morgan Chase Bank. The unidentified male opened the rear cargo area of the vehicle and placed the suitcase and the duffel bag into the vehicle. Agents followed the vehicle to the Hilton Garden Inn – Milwaukee Airport located at 5890 South Howell Avenue, Milwaukee, Wisconsin, where the unidentified male exited the vehicle and entered the hotel.

33. According to JP Morgan Chase Bank records, on November 24, 2020, the unidentified male had made a cash deposit totaling $169,650 in United States currency to an account held by Redzien, LLC, a business organized in the State of Florida.

34. The authorized signers on the Redzien, LLC account were individuals having the initials K.M. and H.M.T.V. Banking records for the Redzien, LLC account show that the account was opened on September 23, 2020.

35. A search of Florida corporation records identified the registered agent for Redzien, LLC as K.M. of 10XXX West Sample Road #4XXX, Coral Springs, Florida. The Articles of Organization for Redzien, LLC identify K.M. and H.M.V. (a.k.a. H.M.T.V.), as managers of the LLC.[5]

36. Banking records identified K.M.'s phone number as (941) 809-5XXX and H.M.T.V.'s phone number as (832) 212-3XXX. T-Mobile records show the subscriber to (941)

[5] Records further show that Redzien, LLC was administratively dissolved on September 24, 2021.

809-5XXX was Conceptual Design & Consulting Srvcs Inc. in North Venice, Florida, and the customer's name as "MXXXXX" (the last name of K.M.). T-Mobile records showed the subscriber to (832) 212-3XXX as "HXXXXX TXXXX" (a portion of the name of H.M.T.V.) in Sanford, Florida. Telephone records further show that K.M., using (941) 809-5XXX, was in regular and frequent contact with K.M.T.V., using (832) 212-3XXX.

37. Bank records show that Redzien, LLC had also opened bank accounts at Bank of America, Wells Fargo Bank, and Regions Bank. Records from those three banks and JP Morgan Chase Bank show approximately 106 suspicious transactions totaling $21,268,257 from June 18, 2020, through March 24, 2021. These transactions occurred in at least twenty-one different states, including Wisconsin.

38. On January 20, 2021, agents spoke to a representative of Bank of America's Global Financial Crimes Investigations – Anti-Money Laundering department. The representative advised that from November 23, 2020, through January 5, 2021, K.M. and H.M.T.V. had deposited approximately $1,000,000 into accounts at Bank of America. Bank of America subsequently closed those accounts due to suspicions that the accounts were being used for money laundering.

39. Records show that soon after these deposits were made, money was wired out of the accounts to brokerage accounts of companies in Mexico and the British Virgin Islands. The brokerage firms that received these wires had previously been identified as being involved in money laundering in numerous drug trafficking and money laundering investigations being conducted by the Drug Enforcement Administration ("DEA"). Furthermore, agents had identified a large amount of cryptocurrency deposits and subsequent transactions made by H.M.T.V. on the cryptocurrency exchange Binance.

40. According to records at the Hilton Garden Inn – Milwaukee Airport, K.M. had rented room 339 for one night on November 24, 2020. K.M. checked into the room at approximately 4:52 p.m., the same time that the agents had observed the Uber drop the unidentified male off at the hotel. K.M. had checked out of the hotel at approximately 3:42 a.m. on November 25, 2020.

41. Based on their training and experience, and the investigation to date, agents believe – based on the numerous large cash deposits followed by wire transfers to foreign accounts, travel throughout the United States in furtherance of money laundering, and the lack of a legitimate business purpose for large cash transactions involving Redzien, LLC (a purported mining business) – that K.M. and H.M.T.V. were involved in laundering drug proceeds throughout the United States, including in the Eastern District of Wisconsin.

Identification of individual having initials L.E.O.T. as leader of a drug trafficking and money laundering organization

42. T-Mobile records for (832) 212-3XXX, used by H.M.T.V., show that H.M.T.V. was in frequent and regular contact with Mexican phone number +52 331 278 6XXX. Open records revealed a July 12, 2019, Facebook post by an individual having the initials L.E.O.T., who had described a lost cat and provided L.E.O.T.'s phone number as +52 331 278 6XXX therein.

43. Open records show that L.E.O.T. was associated with Grupo Gueratti, an investment management company based in Guadalajara, Jalisco, Mexico. Records also show that L.E.O.T. was associated with Twitter account @netogXXXXXXX, an account that frequently discussed and promoted cryptocurrency, including a May 29, 2020, post stating, "The largest Crypto Exchange Worldwide. BINANCE."

44. Based on their training and experience, and the investigation to date, agents believe L.E.O.T. was involved in cryptocurrency transactions with H.M.T.V.

45. Beginning in approximately July 2021, a confidential source ("CS-1") began providing information to agents about the L.E.O.T. drug trafficking and money laundering organization ("DTMLO").

A. CS-1 told investigators that L.E.O.T. was a DTMLO leader who resided in Mexico City and Guadalajara, Mexico, and had been laundering drug proceeds since at least June 2020.

B. CS-1 stated that in the past L.E.O.T. had asserted that L.E.O.T.'s DTMLO laundered proceeds for Colombian- and Mexican-based drug trafficking and money laundering organizations that had cells operating in countries around the world, including the United States.

C. CS-1 confirmed that H.M.T.V. received money pickup contracts from L.E.O.T.

46. CS-1 was able to insert themself as a person capable of fulfilling money pickup[6] contracts in the United States, converting bulk currency to cryptocurrency, and delivering the cryptocurrency to its desired location.

47. In September 2021, CS-1 began receiving money-laundering contracts from L.E.O.T. and L.E.O.T.'s sub-brokers, one of whom was an individual having the initials J.D.L.R.[7]

A. At the direction of agents, CS-1 organized pickups of bulk cash in various cities across the United States, which cash was then deposited into undercover Attorney General Exempt Operation ("AGEO") accounts.[8]

B. After the bulk cash was deposited into undercover bank accounts, it was converted to stablecoin and sent to cryptocurrency deposit addresses provided by L.E.O.T. and/or J.D.L.R.

[6] A money pickup occurs when, in this case, a Mexico-based money broker offers a contract to someone to pick up suspected drug proceeds in the United States, minus a commission, convert it to cryptocurrency, and transfer the cryptocurrency to the money broker.

[7] CS-1 was introduced to J.D.L.R. through L.E.O.T.

[8] AGEO accounts provide DEA the authority to conduct undercover financial transactions to infiltrate and dismantle DTMLOs.

C. In addition to CS-1 completing money contracts on behalf of L.E.O.T. and/or J.D.L.R., information obtained from L.E.O.T. and/or J.D.L.R. money pickups resulted in multiple seizures and/or arrests.

Money laundering contracts with CS-1

48. On or around September 15, 2021, L.E.O.T. offered CS-1 a money laundering contract to pick up approximately $200,000 in United States currency in Dallas, Texas, convert the United States currency to USDT, and transfer it to a USDT address provided by L.E.O.T. At the direction of agents, CS-1 accepted the contract, and Milwaukee DEA agents coordinated with DEA agents in Dallas, Texas, to complete the money pickup.

A. DEA agents in Texas, using an undercover agent ("UC"), were telephonically contacted by an unknown male to arrange for the pickup. This unknown male directed the UC to a home improvement store in Dallas, Texas.

B. On September 17, 2021, DEA agents in Texas established surveillance in the area of the pre-determined location. Surveilling agents saw a male, later identified as an individual having the initials V.J.G., exit his vehicle and provide the UC with a bag determined to contain $199,970 in United States currency.

C. On September 17, 2021, the $199,970 received from V.J.G. was then deposited into a DEA undercover account, converted to USDT, and sent to a deposit address, as directed by L.E.O.T. through CS-1.

49. On October 6, 2021, L.E.O.T. again offered a money laundering contract to CS-1 in Dallas, Texas. The information was passed to DEA Texas agents to assist in the pickup.

A. On October 7, 2021, a DEA Texas UC arranged to pick up approximately $200,000 from V.J.G.

B. V.J.G. was stopped in his vehicle en route to the money pickup for a traffic violation. A consent search of the vehicle was conducted, resulting in the seizure of $199,810 in United States currency.

C. V.J.G. agreed to a search of his residence, resulting in the seizure of seven kilograms of cocaine and an additional $129,500 in United States currency.

50. In September 2023, CS-1 met with J.D.L.R. and an individual having the initials D.A.C.R. in Bogota, Colombia, to discuss future money laundering contracts. During the meeting, J.D.L.R. explained that J.D.L.R. was working for a group from Culiacan, Mexico, and getting the majority of his work from D.A.C.R. D.A.C.R. told CS-1 that D.A.C.R. was sending large amounts of cocaine to various cities in the United States and giving customers 90 days to return the payment through J.D.L.R. D.A.C.R. told CS-1 that D.A.C.R. was looking for USDT transfers and cash payouts in Guayaquil, Ecuador, among other places.

51. Between about September 2021 and about April 2024, at the direction of L.E.O.T., CS-1 had conducted more than 20 money laundering contracts resulting in cryptocurrency transfers for L.E.O.T.'s DTMLO. As part of these contracts, L.E.O.T. had provided CS-1 with several USDT deposit addresses to send USDT.

Binance records for L.E.O.T.'s Binance account

52. Records for the Binance account belonging to L.E.O.T. from May 29, 2020 (the date the account was created) through September 27, 2023, show that the user had deposited 15,617,784.71 BUSD[9] (mainly USDT, USDC[10] & BTC[11]) through 452 cryptocurrency deposits and had withdrawn 15,664,456.29 BUSD (mainly in USDT, XRP[12] & BTC) through 567 cryptocurrency withdrawals. There were 81 OTC[13] trades (USDT most common market) that were

[9] BUSD is a stablecoin issued by Binance, a cryptocurrency exchange. As a stablecoin, BUSD is designed to maintain a stable value of one United States dollar per BUSD token.

[10] USDC, or USD Coin, is a digital stablecoin pegged to the U.S. dollar.

[11] BTC, or Bitcoin, is a digital de-centralized cryptocurrency.

[12] XRP, or Ripple, is a digital de-centralized cryptocurrency.

[13] An OTC trade, or Over-the-Counter trade, is a financial framework that enables trading markets outside a regular exchange. It involves the direct exchange of cryptocurrency assets between two parties within a private trading environment.

made sporadically between transactions, no completed P2P[14] trades, and 330 trades orders filled in USDT markets.

53. Comparing deposits and withdrawals from October 2022 through April 2023, the user's transactions had noticeably common patterns, such as: (1) once the user received deposits in the Binance account, normally it took less than 24 hours for the user to withdraw the same/similar amounts to different addresses leaving the account with a low or zero balance; and (2) the user crossed the funds between blockchain networks, i.e., if the user received the funds in TRX network, the user withdrew the funds in ETH network or vice versa.

54. This behavior confirmed that the user was using Binance as a bridge to change the assets in another blockchain network for an unknown purpose, and the user was not interested in holding/saving the funds, trading, etc.

55. Furthermore, the user was connected to 58 different Binance users by funds flow. These users had different countries of residence, with Mexico and Colombia being the more common countries. Seven of these users were off-boarded[15] for violating Binance's Terms of Use.

56. Given this suspicious transaction activity, the high cryptocurrency amounts managed with unknown sources of wealth, the risky connections (users) by funds flow, the similar pattern observed in other Mexican users investigated, and the diverse law-enforcement requests focused on user's transactions, there was a high probability that the user's activities were related to money laundering, and the user was using Binance to obfuscate the origin of the funds by swapping the assets between networks.

[14] P2P, or peer-to-peer, is an exchange of cryptocurrency assets without the services of an intermediary.
[15] When Binance "off-boards" a user, it means they are completely removing the user's access to their account on the platform, essentially closing their account due to potential violations of Binance's terms of service, often related to concerns about money laundering, fraud, etc.; effectively preventing them from trading or accessing their funds on the exchange.

57. Agents identified a second confidential source ("CS-2") as a Binance user connected to the L.E.O.T. Binance account via funds flow analysis.

58. Analysis of CS-2's Binance account showed similar patterns as those of L.E.O.T.'s Binance account, consistent with money laundering.

Money laundering contracts with CS-2

59. In November 2023, CS-2 stated that he/she was involved in cryptocurrency arbitrage, the buying of a cryptocurrency in one market and selling in another market to make a profit. CS-2 stated the current trend was to purchase USDT from Mexico-based groups at a cheaper rate than the market price, and then sell the USDT in Colombia at Casa de Cambios, virtual currency exchanges, over-the-counter (OTC) transactions, or peer-to-peer transactions (P2P). The USDT was sold at a cheaper rate in Mexico because it was known to be drug proceeds. CS-2 stated there were large amounts of USDT in Culiacan, Guadalajara, and Mexico City, Mexico.

60. CS-2 was able to insert themself as a person capable of fulfilling money pickup contracts in the United States, converting the bulk currency to cryptocurrency, and delivering the cryptocurrency to its desired location. In April 2024, CS-2 began to receive money-laundering contracts from an individual having a first-name initial of "E," a Cali, Colombia-based money broker.

61. On or around April 17, 2024, "E" offered CS-2 a money laundering contract to pick up approximately $80,000 in United States currency in New York, New York, convert the United States currency to USDT, and transfer the USDT to a USDT address provided by "E." At the direction of agents, CS-2 accepted the contract, and Milwaukee DEA agents coordinated with DEA agents in Newark, New Jersey to complete the money pickup.

A. DEA agents in New Jersey, using an undercover agent (UC) and confidential source, were telephonically contacted by an unknown male to arrange for the pickup.

B. On April 18, 2024, the DEA New Jersey confidential source met with an individual having the initials B.B.G. in Brooklyn, New York, and received a black plastic shopping bag containing rubber-banded bundles of United States currency totaling $98,800.

C. On April 18, 2024, the $98,800 in United States currency received from B.B.G. was then deposited into a DEA undercover account, converted to USDT, and 94,759.577574 USDT was sent to a Binance-hosted address ending in c1e6566d, as directed by "E" through CS-2.

62. On May 1, 2024, "E" offered CS-2 a money laundering contract to pick up approximately $100,000 in United States currency in New York, New York. At the direction of agents, CS-2 accepted the contract, and Milwaukee DEA agents coordinated with DEA New Jersey agents.

A. A DEA New Jersey UC and B.B.G. agreed to meet in Brooklyn, New York on May 2, 2024. The UC recognized B.B.G.'s telephone number as the same number used in the April 18, 2024, money pickup.

B. On May 2, 2024, DEA New Jersey agents established surveillance in the immediate vicinity of the meet location and B.B.G.'s residence. Agents saw a male, later identified as B.B.G.'s brother, carry a weighted black shopping bag to B.B.G.'s vehicle.

C. Agents approached the brother and asked what was in the bag, to which the brother replied "money." The brother opened the bag, and agents saw bundles of United States currency wrapped in rubber bands.

D. B.B.G. then exited his home and admitted to agents that he was the owner of the money and had asked his brother to drop off the money in his favor. B.B.G. confirmed the money was approximately $100,000 to be dropped off in Brooklyn and that he had more money inside his house.

E. B.B.G. gave agents verbal and written consent to search his home. Upon searching the home, agents located approximately $150,000 in United States currency bundled in rubber bands, which currency was suspected narcotics proceeds.

Address Mbc25MQY's involvement in the money laundering operation (address Mbc25MQY is the address from which the defendant approximately 2,155,760.485382 Tether (USDT) cryptocurrency was seized)

63. Binance records for the deposit address ending in c1e6566d (to which approximately 94,759 USDT had been transferred on April 18, 2024, from a money laundering contract, as noted in paragraph 61) show the address was associated with Binance user ID ending in 9395, which was registered to an individual having the initials J.C.C.B. According to IP login information, J.C.C.B. commonly logged in from Ibague, Colombia.

64. Records further show that on April 18, 2024, 94,752 USDT was sent from J.C.C.B.'s Binance account via the Tron network to an address ending in jHXdrumo.

65. Agents traced the 94,752 USDT on the Blockchain as it made several "hops" in a short period of time, before a portion of it (approximately 50,000 USDT) landed in an unhosted wallet as follows:

A. On April 18, 2024, 93,916 USDT was sent from jHXdrumo to an address ending in YLaJm7Ra;

B. On April 18, 2024, a total of 94,239 USDT was sent from YLaJm7Ra in two transactions: (1) 13,700 USDT to an address ending in vrsXeBD7, and (2) 80,539 USDT to an address ending in PmX9vVF7;

C. On April 19, 2024, 78,300 USDT was sent from PmX9vVF7 to an address ending in DWbWeBcz;

D. On April 19, 2024, and April 23, 2024, a total of 75,443 USDT was sent from DWbWeBcz in two transactions: (1) 50,000 USDT to an address ending in h7v7afHx (April 19, 2024), and (2) 25,443 USDT to an address ending in eNyQNbH9 (April 23, 2024);

E. On April 22, 2024, 50,940 USDT was sent from h7v7afHx to an address ending in nhGBSxQ8;

F. On April 22, 2024, 51,000 USDT was sent from nhGBSxQ8 to an address ending in Y7caRNRq; and

G. On April 23, 2024, Y7caRNRq combined the 51,000 USDT with other deposits and sent 197,880 USDT to an address ending in Mbc25MQY ("address Mbc25MQY"), which is the address from which the defendant approximately 2,155,760.485382 Tether (USDT) cryptocurrency was seized.

66. Agents analyzed the several "hop" deposit addresses through which the USDT from the April 18, 2024 New York money pickup had moved and found the addresses all had minimal balances of cryptocurrency. Based on their training and experience, and the investigation to date, agents believe these accounts were "pass through" accounts, meaning the accounts were merely used to pass the cryptocurrency from one address to another, to obfuscate the source of the funds.

67. Once the USDT from the April 18, 2024 New York money pickup arrived at address Mbc25MQY, the funds remained in the account while other suspicious deposits arrived. Agents analyzed address Mbc25MQY and found approximately $22,444,554 in cryptocurrency had been sent to the account, with approximately $20,291,798 having been withdrawn from the account, between March 15, 2024, and April 26, 2024.

68. Address Mbc25MQY was categorized as an unhosted wallet, meaning it was not connected to a virtual currency exchange that would require Know Your Customer ("KYC")[16] information. Based on their training and experience, and the investigation to date, agents know that money launderers commonly use unhosted wallets to remain anonymous and avoid law enforcement detection.

[16] KYC is the process that banks and other financial institutions use, in part, to verify a customer's identity when opening an account.

Binance 7382's involvement in the money laundering operation (Binance 7382 is the account from which the defendant approximately 114,366.044785 Tether (USDT) cryptocurrency was seized)

69. With an unhosted wallet, a user needs "gas" to send USDT via the Ethereum or Tron network. Gas is the fee required to successfully conduct a transaction or execute a contract on the Ethereum or Tron blockchain platform. By following the trail related to "gas fees," agents can connect individuals associated with the unhosted wallet because "gas fees" can generally be traced to a virtual currency exchange that requires KYC.

70. According to records for address Mbc25MQY, the first "gas fee" transaction was an incoming transfer of 791.5067 TRX cryptocurrency on March 15, 2024, from an address ending in QQMUxHLS associated with Binance. Binance records show that the transfer came from Binance account user ID ending in 7382 ("Binance 7382") registered to J.M.U.L. According to IP login information, J.M.U.L. commonly logged in from Culiacan, Mexico, and other locations in Mexico.

71. Binance records show that Binance 7382 sent "gas fees" for other unhosted wallets, including the transfer of 0.007679 ETH cryptocurrency to an address ending in 459DAF53 ("address 459DAF53") on March 15, 2024.

72. From January 27, 2024, until June 27, 2024, Binance 7382 received 209 incoming deposits totaling approximately 6,079,090 USDT.

73. From January 29, 2024, until June 27, 2024, Binance 7382 sent out 192 withdrawals, totaling approximately 3,685,260 USDT.

74. Binance 7382 also conducted approximately 187 "taker sell" peer-to-peer (P2P) transactions totaling approximately 2,171,895 USDT.

75. Records for Binance 7382 show characteristics of money laundering activity, including but not limited to the following:

A. Rapid movement of cryptocurrencies into and out of the account over short periods of time;

B. Large dollar equivalent amounts of cryptocurrency transactions in and out of the account that often, but not always, result in a near net zero or relatively small dollar ending balance; and

C. A flow of cryptocurrency funds to user accounts owned by individuals in narcotic source countries (e.g., Mexico and Colombia), consistent with transactions that DEA has observed in undercover operations.

Binance 7382 linked to additional money laundering investigations

76. Records for address 459DAF53 showed several deposits tied to additional law enforcement investigations. Some of those transactions included the following:

A. In March 2024, two deposits from undercover law enforcement accounts to address 459DAF53 – the address "gassed up" by J.M.U.L.'s Binance 7382 – were as follows: 109,583.46461 USDT to address 459DAF53 on March 15, 2024; and 94,434.083713 USDT to address 459DAF53 on March 18, 2024.

B. On April 10, 2024, DEA agents in Baltimore, Maryland, picked up approximately $99,000 in cash based on a money pickup contract provided by DEA agents in Denver, Colorado, through a Mexico-based money broker. On April 11, 2024, DEA undercover agents sent 94,545 USDT to address 459DAF53, the address "gassed up" by J.M.U.L.'s Binance 7382.

C. On April 11, 2024, DEA agents in Atlanta, Georgia, picked up approximately $100,000 in cash based on a money pickup contract provided by DEA agents in Denver, Colorado, through a Mexico-based money broker. On April 12, 2024, DEA undercover agents sent 95,429.395405 USDT to address 459DAF53, the address "gassed up" by J.M.U.L.'s Binance 7382.

D. On April 16, 2024, DEA agents in Minneapolis, Minnesota, picked up approximately $199,800 in cash from a money courier based on a contract provided by DEA agents in Denver, Colorado, through a Mexico-based money broker. On April 17, 2024, DEA undercover agents sent 190,682.974469 USDT to address 459DAF53, the address "gassed up" by J.M.U.L.'s Binance 7382. In addition, on April 17, 2024, DEA Minneapolis

executed a State of Minnesota search warrant and seized approximately $257,396, drug notes, packaging items, and one ounce of an unknown white powdery substance from that courier.

77. Records show that three of the transactions identified in paragraph 76 were sent to J.M.U.L.'s Binance 7382 as follows:

A. On March 15, 2024, 108,424 USDT was sent from address 459DAF53 to Binance 7382.

B. On April 11, 2024, 94,440 USDT from the DEA Baltimore contract was sent from address 459DAF53 to Binance 7382.

i. Further tracing of this 94,440 USDT sent from address 459DAF53 to Binance 7382, shows that on April 12, 2024, Binance 7382 sent 100,000 USDT to an address ending in yGnx2aaf ("address yGnx2aaf").

ii. Address yGnx2aaf combined this 100,000 USDT deposit from Binance 7382 with other suspicious deposits (including an additional 193,633 USDT from Binance 7382), and on April 15, 2024, sent 591,100 USDT to an address ending in XkPYyCSJ ("address XkPYyCSJ"), which is the address from which the defendant approximately 3,314,499.122779 Tether (USDT) cryptocurrency was seized.

iii. Between April 12, 2024, and April 29, 2024, Binance 7382 sent six transactions totaling 565,657 USDT to address yGnx2aaf.

iv. On April 19, 2024, address yGnx2aaf sent 544,900 USDT to address XkPYyCSJ, which is the address from which the defendant approximately 3,314,499.122779 Tether (USDT) cryptocurrency was seized.

C. On April 17, 2024, 190,723 USDT from the DEA Minneapolis contract was sent from address 459DAF53 to Binance 7382.

78. Records show that address yGnx2aaf was an unhosted wallet, meaning it was not connected to a virtual currency exchange that would require KYC information. Based on their training and experience, and the investigation to date, agents know that money launderers commonly use unhosted wallets to remain anonymous and avoid law enforcement detection.

79. Between March 21, 2024, and June 13, 2024, records show that address yGnx2aaf had 224 incoming transfers totaling approximately $5,080,031 in cryptocurrency and 28 outgoing transfers totaling approximately $5,079,959 in cryptocurrency. Based on their training and experience, and the investigation to date, agents believe address yGnx2aaf was used by the money laundering organization to "pool" suspicious deposits before sending them to another deposit address.

Address XkPYyCSJ's involvement in the money laundering operation (address XkPYyCSJ is the address from which the defendant approximately 3,314,499.122779 Tether (USDT) cryptocurrency was seized)

80. Address XkPYyCSJ (to which 591,100 USDT and 544,900 USDT had been transferred on April 15, 2024, and April 19, 2024, respectively, from address yGnx2aaf, as noted in paragraphs 77Bii and 77Biv) was categorized as an unhosted wallet, meaning it was not connected to a virtual currency exchange that would require KYC information. Based on their training and experience, and the investigation to date, agents know that money launderers commonly use unhosted wallets to remain anonymous and avoid law enforcement detection.

81. Records for address XkPYyCSJ show that from March 19, 2024, through April 26, 2024, there were approximately $5,406,678 of incoming cryptocurrency transfers and approximately $2,093,430 in outgoing cryptocurrency transfers.

82. Records for address XkPYyCSJ further show that address Mbc25MQY (the address from which the defendant approximately 2,155,760.485382 Tether (USDT) cryptocurrency was seized) sent three transactions to address XkPYyCSJ – namely, 800,000 USDT on April 4, 2024; 193 USDT on April 13, 2024; and 1,844,000 USDT on April 13, 2024 – with a total value of approximately $2,643,740.

83. Based on the investigation to date, agents believe address XkPYyCSJ was in the same money laundering network as address Mbc25MQY and was also connected to transactions made by J.M.U.L. For example:

A. J.M.U.L.'s Binance 7382 account received two incoming transfers from address ending in xAcFyEDX (address xAcFyEDX) – namely, 288,000 USDT on March 1, 2024; and 16,000 USDT on March 5, 2024.

B. Between January 2024 and May 2024, J.M.U.L.'s Binance 7382 account sent four transfers totaling 198,670 USDT to address xAcFyEDX.

C. On April 23, 2024, address xAcFyEDX sent 100 USDT to address XkPYyCSJ.

D. On April 24, 2024, address xAcFyEDX sent 163,900 USDT to address XkPYyCSJ.

84. Records show that between March 21, 2024, and May 9, 2024, address xAcFyEDX was also involved in transactions with address yGnx2aaf (the address referenced in paragraphs 77-79) totaling approximately $1,140,000 in incoming and outgoing transactions.

85. Based on their training and experience, and the investigation to date, agents believe that address Mbc25MQY, address XkPYyCSJ, and Binance 7382 – from which the defendant properties were seized – were used to "pool" suspicious transactions before large withdrawals were made.

86. Based on their training and experience, and the investigation to date, agents believe that J.M.U.L. and others used unhosted wallets, including address Mbc25MQY (from which the defendant approximately 2,155,760.485382 Tether (USDT) cryptocurrency was seized) and address XkPYyCSJ (from which the defendant approximately 3,314,499.122779 Tether (USDT) cryptocurrency was seized), to avoid law enforcement detection, remain anonymous, and to launder "dirty" cryptocurrency.

87. Based on their training and experience, and the investigation to date, agents believe that address Mbc25MQY, address XkPYyCSJ, and Binance 7382 – from which the defendant properties were seized – were involved in an international money laundering operation connected to J.M.U.L. and others.

Warrant for Arrest In Rem

88. Upon the filing of this complaint, the plaintiff requests that the Court issue an arrest warrant *in rem* pursuant to Supplemental Rule G(3)(b), which the plaintiff will execute upon the defendant properties pursuant to 28 U.S.C. § 1355(d) and Supplemental Rule G(3)(c).

Claim for Relief

89. The plaintiff repeats and incorporates by reference the paragraphs above.

90. By the foregoing and other acts, the defendant property, approximately 114,366.044785 Tether (USDT) cryptocurrency from Binance account user ID ending in 7382, represents proceeds of distribution of controlled substances and a conspiracy to distribute, manufacture, dispense, or possess with the intent to manufacture, distribute, or dispense controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846.

91. The defendant approximately 114,366.044785 Tether (USDT) cryptocurrency from Binance account user ID ending in 7382 is therefore subject to forfeiture to the United States of America under 21 U.S.C. § 881(a)(6).

92. By the foregoing and other acts, the defendant property, approximately 114,366.044785 Tether (USDT) cryptocurrency from Binance account user ID ending in 7382, (1) was involved in, or is traceable to funds involved in, money laundering transactions and a conspiracy to engage in money laundering in violation of 18 U.S.C. §§ 1956 and 1957; and (2) was

involved in, or is traceable to funds involved in, unlicensed money transmitting in violation of 18 U.S.C. § 1960.

93. The defendant approximately 114,366.044785 Tether (USDT) cryptocurrency from Binance account user ID ending in 7382 is therefore subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 984.

94. By the foregoing and other acts, the defendant property, approximately 2,155,760.485382 Tether (USDT) cryptocurrency from cryptocurrency address ending in Mbc25MQY, represents proceeds of distribution of controlled substances and a conspiracy to distribute, manufacture, dispense, or possess with the intent to manufacture, distribute, or dispense controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846.

95. The defendant approximately 2,155,760.485382 Tether (USDT) cryptocurrency from cryptocurrency address ending in Mbc25MQY is therefore subject to forfeiture to the United States of America under 21 U.S.C. § 881(a)(6).

96. By the foregoing and other acts, the defendant property, approximately 2,155,760.485382 Tether (USDT) cryptocurrency from cryptocurrency address ending in Mbc25MQY, (1) was involved in, or is traceable to funds involved in, money laundering transactions and a conspiracy to engage in money laundering in violation of 18 U.S.C. §§ 1956 and 1957; and (2) was involved in, or is traceable to funds involved in, unlicensed money transmitting in violation of 18 U.S.C. § 1960.

97. The defendant approximately 2,155,760.485382 Tether (USDT) cryptocurrency from cryptocurrency address ending in Mbc25MQY is therefore subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 984.

98. By the foregoing and other acts, the defendant property, approximately 3,314,499.122779 Tether (USDT) cryptocurrency from cryptocurrency address ending in XkPYyCSJ, represents proceeds of distribution of controlled substances and a conspiracy to distribute, manufacture, dispense, or possess with the intent to manufacture, distribute, or dispense controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846.

99. The defendant approximately 3,314,499.122779 Tether (USDT) cryptocurrency from cryptocurrency address ending in XkPYyCSJ is therefore subject to forfeiture to the United States of America under 21 U.S.C. § 881(a)(6).

100. By the foregoing and other acts, the defendant property, approximately 3,314,499.122779 Tether (USDT) cryptocurrency from cryptocurrency address ending in XkPYyCSJ, (1) was involved in, or is traceable to funds involved in, money laundering transactions and a conspiracy to engage in money laundering in violation of 18 U.S.C. §§ 1956 and 1957; and (2) was involved in, or is traceable to funds involved in, unlicensed money transmitting in violation of 18 U.S.C. § 1960.

101. The defendant approximately 3,314,499.122779 Tether (USDT) cryptocurrency from cryptocurrency address ending in XkPYyCSJ is therefore subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 984.

WHEREFORE, the United States of America prays that a warrant of arrest for the defendant properties be issued; that due notice be given to all interested parties to appear and show cause why the forfeiture should not be decreed; that judgment declare the defendant properties to be condemned and forfeited to the United States of America for disposition according to law; and that the United States of America be granted such other and further relief as this Court may deem just and equitable, together with the costs and disbursements of this action.

Dated at Milwaukee, Wisconsin, this 20th day of November, 2024.

Respectfully submitted,

GREGORY J. HAANSTAD
United States Attorney

By: *s/Elizabeth M. Monfils*

ELIZABETH M. MONFILS
Assistant United States Attorney
Wisconsin Bar No. 1061622
Office of the United States Attorney
Eastern District of Wisconsin
517 E. Wisconsin Avenue, Room 530
Milwaukee, WI 53202
Telephone: (414) 297-1700
Fax: (414) 297-1738
E-Mail: elizabeth.monfils@usdoj.gov

Verification

I, Kellen Williams, hereby verify and declare under penalty of perjury that I am a Special Agent with the Drug Enforcement Administration ("DEA"), that I have read the foregoing Verified Complaint for Civil Forfeiture *in rem* and know the contents thereof, and that the factual matters contained in paragraphs 18 through 87 of the Verified Complaint are true to my own knowledge.

The sources of my knowledge are the official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Agent with the DEA.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Date: 11/19/2024

s/Kellen Williams
Kellen Williams
Special Agent
Drug Enforcement Administration